IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**chsknoxville@gmail.com [1]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**lucasartini@gmail.com [2]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**bensfmc@gmail.com [3]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**shofstetter4@gmail.com [4]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

Case No. 3:18 MJ 1026 – 3:18 MJ 1043

**Filed Under Seal**

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**nicole.sfmcdeco@gmail.com [5]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**maynardalvarez1522@gmail.com [6]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**pain6100@gmail.com [7]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**jimmypalmamd@gmail.com [8]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**webbankus@gmail.com [9]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**filipposantonocito@yahoo.it [10]**

THAT IS STORED AT PREMISES CONTROLLED BY Oath Holdings Inc., 701 First Avenue, Sunnyvale, CA 94089.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**shofstetter4@yahoo.com [11]**

THAT IS STORED AT PREMISES CONTROLLED BY Oath Holdings Inc., 701 First Avenue, Sunnyvale, CA 94089.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**jimmypalmamd@aol.com [12]**

THAT IS STORED AT PREMISES CONTROLLED BY Oath Inc., 22000 AOL Way, Dulles, VA 20166.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**andrew@911urgent.com [13]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**ben@911urgent.com [14]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**CTipton@911urgent.com [15]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH

**luca@911urgent.com [16]**

THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

---

| |
|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH<br><br>**sylvia@911urgent.com [17]**<br><br>THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043. |
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH<br><br>**medfix@911urgent.com [18]**<br><br>THAT IS STORED AT PREMISES CONTROLLED BY Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043. |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Steven P. Haughton being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are cited above, and are stored at premises controlled by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, Oath Holdings Inc., an email provider located at 701 First Avenue, Sunnyvale, CA 94089 (formerly known as Yahoo Holdings, Inc.), and Oath Inc., an email provider located at 22000 AOL Way, Dulles, VA 20166 (formerly known as AOL, Inc. c/o Oath

Inc.)[1]. Through the remainder of this Affidavit, the requested email providers (Email Providers) refers to the Email Providers cited above, and the requested accounts (Requested Accounts) refers to the accounts cited above. The information to be searched for is described in the following paragraphs and in Attachments A-1 to A-4 for each Email Provider. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Email Providers to disclose to the government copies of the information (including the content of communications) further described in the following Section I of Attachments B-1 through B-4 for each Requested Account. Upon receipt of the information described in Section I of Attachments B-1 through B-4, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-4.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since 2008. During my career as a Special Agent, I have investigated criminal violations that involved drug trafficking, terrorism, online child exploitation, and computer intrusions. Many of these investigations involved the use of email and the internet. Also, I have received training from the FBI Academy regarding the use of email in criminal investigations, and possess A+ and Net+ certifications which are industry recognized certifications for information technology professionals.

3. This affidavit is intended to show there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

---

[1] When Verizon acquired Yahoo, Inc. in April 2017, it merged Yahoo and AOL into the new name Oath Inc. On March 7, 2018, FBI personnel were notified to serve legal process for Yahoo to Oath Holdings Inc., and legal process for AOL to Oath Inc.

4. Based on my training and experience and the facts as set forth in this affidavit, my personal knowledge of this investigation, and information shared with me by other investigators working on this investigation, there is probable cause to believe that violations of 18 U.S.C. Section 1962 (Racketeering Influenced and Corrupt Organizations Act), 21 U.S.C. Section 841 (Illegal Dispensing of Controlled Substances), 21 U.S.C. Section 846 (Drug Trafficking Conspiracy), 18 U.S.C. Sections 1956 and 1957 (Money Laundering), 21 U.S.C. Section 856 (Drug-involved Premises), and 18 U.S.C. Section 371 and 42 U.S.C. 1320a-7b(b)(1)(A) (conspiracy to solicit healthcare kickbacks), have been committed by the defendants and subjects listed below. Collectively, these offenses are referred to as the subject offenses throughout the rest of this Affidavit. There is also probable cause to search the Requested Accounts, described in Attachments A-1 through A-4 for evidence of these crimes, more fully described in Attachments B-1 through B-4.

## JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

## PROBABLE CAUSE

6. Since approximately January 2010, various law enforcement agencies, including the Drug Enforcement Agency (DEA) and FBI, have investigated a group of associated pain clinics in Florida and Tennessee for the illegal distribution of prescription pain medication, to include oxycodone. Urgent Care & Surgery Center, Inc. (the HOLLYWOOD CLINIC) was a pain clinic investigated by the DEA located at 3500 Hollywood Boulevard, Hollywood, Florida.

The HOLLYWOOD CLINIC was incorporated in or about April 2009. For the purpose of establishing probable cause, I have attached the application and affidavit for a search warrant at the HOLLYWOOD CLINIC (Exhibit 1).

7. On or about December 13, 2010, law enforcement executed a search warrant at the HOLLYWOOD CLINIC. In addition to the pain clinic, the HOLLYWOOD CLINIC operated an on-site pharmacy. Leading up to the search, law enforcement conducted approximately fourteen undercover visits to the HOLLYWOOD CLINIC, and successfully obtained prescriptions for approximately 1,890 Oxycodone 30mg tablets, and other controlled substances, without medical necessity. During one visit, a Special Agent acting in an undercover capacity explained to the physician that he was illegally selling his opioid prescription on the streets. The Special Agent was discharged from the clinic, but was still provided a full opioid prescription. However, the Special Agent was not allowed to fill the prescription at the on-site pharmacy.

8. During another visit, a Special Agent, acting in an undercover capacity, heard patients talk about people being arrested for pills, and that one of the patients was in prison for selling his pills. During surveillance of the HOLLYWOOD CLINIC, law enforcement observed that many of the patients were young, few exhibited outward signs of being in chronic pain, and many appeared to be sponsored because they arrived and waited together.

9. Former patients who were interviewed by law enforcement described the HOLLYWOOD CLINIC as a pill mill because it was known as an easy place to get pills. Physicians prescribed pain medication as long as the patients said the right things and had current MRIs. The patients admitted to being addicts. Exams were short, and patients paid in

cash. The HOLLYWOOD CLINIC did not accept insurance for pain patients and charged approximately $200 per office visit, excluding prescription costs.

10. Although the HOLLYWOOD CLINIC was called an urgent care center, one patient reported that she/he did not observe any patients who appeared to be injured, which was corroborated by what law enforcement observed at the clinic. One of the owners of the HOLLYWOOD CLINIC was interviewed by law enforcement. The owner acknowledged that pain management was the dominant business of the HOLLYWOOD CLINIC and the primary source of revenue prior to the search warrant execution in December 2010. After the search warrant execution, the HOLLYWOOD CLINIC began operating much more conservatively and saw significantly fewer patients. As a consequence, the HOLLYWOOD CLINIC's profitability fell dramatically. In contrast, the new pain clinics opened by the owners of the HOLLYWOOD CLINIC in Tennessee after the Florida raid once again generated large revenues and profits totaling millions of dollars. Based on financial records and Florida Secretary of State filings, I believe that the owners sold the HOLLYWOOD CLINIC in or about September 2016.

11. On or about January 4, 2018, a federal Grand Jury sitting in Knoxville returned a Third Superseding Indictment in Case Number 3:15-CR-27 charging the owners and a manager of the Florida and Tennessee clinics (i.e., Luca Sartini, Luigi Palma, Benjamin Rodriguez, and Sylvia Hofstetter) with various offenses, including a Racketeer Influenced and Corrupt Organization (RICO) conspiracy and drug trafficking conspiracy. The alleged dates of the conspiracies, April 2009 through March 10, 2015, encompass the illegal activities of the HOLLYWOOD CLINIC described herein.

12. Based on the aforementioned facts, in conjunction with the attached search warrant affidavit (Exhibit 1) and the Third Superseding Indictment (attached hereto as Exhibit 2),

I believe the HOLLYWOOD CLINIC operated as a pill mill. Generally, the HOLLYWOOD CLINIC did not accept insurance for pain patients, medical exams were unreasonably expensive, brief and superficial, patients were routinely prescribed pain medication without medical necessity, and many patients subsequently abused and/or sold their pills.

13. By late 2010 and early 2011, it was commonly known in South Florida that the pill mill business was coming under increasingly high levels of scrutiny by law enforcement and regulators. Around the same time period, there was a change in Florida law generally requiring pain clinics to be owned by physicians instead of lay business people. Shortly prior to the December 2010 search warrant execution at the HOLLYWOOD CLINIC, SARTINI, PALMA, and/or RODRIGUEZ caused the HOLLYWOOD CLINIC's articles of incorporation to be changed by removing SARTINI, PALMA, and RODRIGUEZ as directors, and replacing them with Eric O. Pantaleon M.D. as the new director. Approximately nine days after the December 2010 DEA search, SARTINI, PALMA, and/or RODRIGUEZ caused MEDFIX, LLC (MEDFIX) to be established as a business entity through which SARTINI, PALMA, and RODRIGUEZ continued to control the HOLLYWOOD CLINIC despite the recently revised articles of incorporation naming PANTALEON as the new director. Regardless of how the HOLLYWOOD CLINIC was structured, staff and other witnesses understood that SARTINI, PALMA, and RODRIGUEZ were the true owners. RODRIGUEZ's wife, Nicole Rodriguez (NICOLE RODRIGUEZ) also worked at the HOLLYWOOD CLINIC, and was listed as a managing member of MEDFIX.

14. In or about late 2010, SARTINI, PALMA, and RODRIGUEZ partnered with Christopher Tipton (TIPTON), and began laying the groundwork to open a new pill mill in Knoxville, Tennessee. Initially, the new clinic was called Urgent Care & Surgery Center, just

like the HOLLYWOOD CLINIC. Later, the name was changed to Comprehensive Healthcare Systems (CHCS-Knoxville). The Florida partners sent Sylvia Hofstetter (HOFSTETTER), who was a former office manager at the HOLLYWOOD CLINIC, to run CHCS-Knoxville. Later, CHCS opened another clinic location in Lenoir City, Tennessee (CHCS-Lenoir City). Following nuisance complaints by other tenants and disputes with the landlord, the partners closed CHCS-Knoxville and consolidated it with CHCS-Lenoir City.

15. In or about January 2013, TIPTON and HOFSTETTER established another pill mill called East Knoxville Healthcare Services (EKHCS) located on Lovell Road in Knoxville. TIPTON and HOFSTETTER opened EKHCS without the knowledge of the Florida partners. HOFSTETTER funneled patients discharged from CHCS-Lenoir City to EKHCS. HOFSTETTER continued to operate CHCS-Lenoir City for SARTINI, PALMA, RODRIGUEZ, and TIPTON. However, HOFSTETTER staffed EKHCS with office workers and medical providers from CHCS-Lenoir City. The medical staff split time between both locations.

16. The FBI began its active investigation of CHCS-Lenoir City and EKHCS in or about 2013. On or about March 10, 2015, following a lengthy investigation involving the use of undercover agents, court-authorized wiretaps, and a financial investigation, law enforcement executed federal search warrants at CHCS-Lenoir City, EKHCS, and HOFSTETTER's Knoxville residence. For the purpose of supporting probable cause for this request, I have attached the affidavit filed in support of the search warrant applications in March 2015. (Exhibit 3).

17. Relevant to this application, agents seized the following items on March 10, 2015, at the locations noted:

a. HOFSTETTER's residence: A Samsung Galaxy Tab tablet computer.

b. CHCS-Lenoir City: Patient charts, other medical records, and business records.

c. EKHCS: Patient charts, other medical records, business records, an Acer EZ Vision laptop computer, and an HP Pavilion desktop computer.

18. For purposes of further establishing probable cause, I have attached the Third Superseding Indictment containing relevant definitions of entities and individuals associated with this investigation (Exhibit 2, pp. 3-11). The following is a non-exhaustive list of additional individuals and entities relevant to this Affidavit and Attachments A-1 to A-4 and B-1 to B-4.

a. Prodigal Primary Care, PC (PRODIGAL), was a company controlled by David Brickhouse (BRICKHOUSE), who is now deceased. In or about 2011, BRICKHOUSE met with SARTINI, PALMA, RODRIGUEZ, and HOFSTETTER at a location in Knoxville, Tennessee. As a result of this meeting, BRICKHOUSE entered into an agreement to send patient referrals to CHCS-Knoxville in exchange for what he understood to be an illegal kickback or bribe. According to BRICKHOUSE, he later changed his mind about the kickbacks, but still referred patients to the Tennessee clinics. BRICKHOUSE eventually sold PRODIGAL to TIPTON, SARTINI, PALMA, and HOFSTETTER.

b. Filippo Santonocito (SANTONOCITO) is an Italian national who periodically lives in Florida, on lawful permanent resident status (LPR). SANTONOCITO received illegal healthcare kickback distributions from GENESIS through an entity called LELF Global Healthcare (LELF). GENESIS was a shell company used by TIPTON to bill STERLING for drug screenings as part of a conspiracy to solicit healthcare kickbacks (See Exhibit 2, p. 7 and p. 60 (start of Count 13). The specimens that were tested by STERLING came from PRODIGAL, CHCS, and

EKHCS. SANTONOCITO also purchased the property that housed one of the PRODIGAL clinics, and received rent payments from Knoxville Healthcare Management (KHM), which was controlled by TIPTON, SARTINI, and HOFSTETTER.

c. Sergio Massaglia (MASSAGLIA) is an associate of SANTONOCITO, SARTINI, and PALMA. The investigation revealed that MASSAGLIA was affiliated with SARTINI in a hair restoration business called Medical Hair Institute Corporation. In July 2015, the FBI received information from Italian law enforcement that MASSAGLIA had an extensive criminal record in Italy. MASSAGLIA's criminal record included complaints for money laundering and grand larceny, as well as a conviction for unlawful financial activities. It appears as though MASSAGLIA used and/or uses various companies and properties he owns as "fronts" for circumventing asset controls. MASSAGLIA went into hiding in 2014, and was believed to have resided in or near Miami, Florida.

d. Andrew Walker (WALKER) was the onsite accountant and business manager of the HOLLYWOOD CLINIC in 2011 and 2012. WALKER also was responsible for compliance with healthcare laws and regulations. WALKER resigned after he became concerned about out-of-state patients visiting the HOLLYWOOD CLINIC, treatment standards, and patients who he believed were doctor shopping (*i.e.*, visiting multiple doctors complaining of the same ailments in an effort to obtain multiple prescriptions for the same or similar drugs). The HOLLYWOOD CLINIC was turning these patients away, but SARTINI, PALMA, and RODRIGUEZ pushed to keep the patients. WALKER did not believe that the

HOLLYWOOD CLINIC was being operated in compliance with the applicable laws and regulations.

19. The FBI investigation in Tennessee resulted in the indictment of over 130 people, including several clinic employees, to include TIPTON and HOFSTETTER. The majority of these individuals pleaded guilty and cooperated with the government. To date, the investigation has included over 350 interviews of patients, staff, employees and others formerly associated with the clinics in Tennessee. The investigation revealed that the clinics were pill mills created to enrich the owners and operators financially through the illegal distribution of medically unnecessary opioid prescriptions, and through illegal kickbacks for laboratory urine drug testing.

20. As part of the investigation, each of the relevant computers identified previously that were seized during the search warrants at the Tennessee locations were forensically processed for review. The review of the information that resulted included email correspondence relevant to the operation of the pill mills or the urine drug screening kickback scheme, and involving or referencing SARTINI, PALMA, RODRIGUEZ, TIPTON, HOFSTETTER, NICOLE RODRIGUEZ, WALKER, SANTONOCITO, and MASSAGLIA. Examples of some of that email correspondence is described below.

a. A review of information from an Acer EZ Vision laptop computer seized from EKHCS on March 10, 2015, revealed an email dated August 6, 2013, from **ctipton@leveragehealthcare.com**, used by TIPTON, to **shofstetter4@gmail.com [4]**, used by HOFSTETTER. The subject of the email reads, "Todds letter." Attached to the email was a letter from the Tennessee Department of Health to physician assistant Todd Stanford that notified him about being one of the top 50 prescribers of opioids in the state. Stanford was instructed

to provide a written explanation justifying the amounts and medical necessity of the controlled substances prescribed. Enclosed with this letter was a summary that reflected a total of 990,349 dosage units of controlled substances prescribed by Stanford. Also attached to this email was the requested response letter. The response from the **shofstetter4@gmail.com [4]** account was, "Thanks. Syl Hofstetter."

b. Based on this email, I believe that the email account **shofstetter4@gmail.com [4]** is controlled by HOFSTETTER and that evidence of the crimes described in this Affidavit are contained in the email account **shofstetter4@gmail.com [4]**. Specifically the email discusses the high level of prescriptions by a clinic provider, which is evidence of the clinic's operation as a pill mill.

c. A review of information from an Acer EZ Vision laptop computer seized from EKHCS on March 10, 2015, revealed an email chain ending on March 12, 2013 from **shofstetter4@gmail.com [4]** to "Connie E. French" at cfrench@fsgbank.com in regard to the "Urgent Care Loan Closing." In the email, HOFSTETTER identified SARTINI's email addresses as **lucasartini@gmail.com [2]**, used by SARTINI, and **chsknoxville@gmail.com [1]**, used by one or more owners and/or employees of CHCS-Knoxville. HOFSTETTER requested that Connie French send the loan papers to both email addresses.

d. Based on this email chain, I believe **lucasartini@gmail.com [2]** is controlled by SARTINI, and that the loan they discussed was taken out by Urgent Care & Surgery Center Management, LLC to purchase the residence at 1842 Falcon Point

Drive, Knoxville, Tennessee 37922. HOFSTETTER lived at the residence and used it as an office to support the operation of the Tennessee pain clinics. Since HOFSTETTER and SARTINI used these email accounts to communicate about a transaction that was relevant to the operation of the pill mills, there is probable cause to believe they corresponded about other aspects of the pill mill operation on these accounts as well.

e. Additionally, an interview of the office manager at EKHCS revealed that patient appointments were scheduled on Google Calendar via the **chsknoxville@gmail.com [1]** account. Based on a forensic review of smart phones and an iPad used by HOFSTETTER, it is apparent that HOFSTETTER utilized Google Calendar frequently from multiple devices. Therefore, I believe the calendar entries linked to this account will contain evidence relevant to patient identification and an analysis of patient volume. Accordingly, I believe that evidence of the crimes described in this Affidavit are contained in the email accounts **lucasartini@gmail.com [2]** and **chsknoxville@gmail.com [1]**.

f. A review of information from an HP Pavilion desktop computer seized from EKHCS on March 10, 2015, revealed an email chain beginning on June 10, 2010, from **pain6100@gmail.com [7]** to **lucasartini@gmail.com [2]**. The chain continues with the addition of emails to **jimmypalmamd@gmail.com [8]** and **bensfmc@gmail.com [3]**, which was reflected in the email header as "Benjamin Rodriguez <bensfmc@gmail.com>" that same day. (See Exhibit 4). An owner or employee of the HOLLYWOOD CLINIC was the most likely user of **pain6100@gmail.com [7]**; SARTINI was the most likely user of

**lucasartini@gmail.com [2]**; PALMA was the most likely user of **jimmypalmamd@gmail.com [8]**; and RODRIGUEZ was the most likely user of **bensfmc@gmail.com [3]**

g. The email chain discussed giving ownership of a clinic to a doctor while maintaining a management contract with that clinic. Based on the name of the doctor discussed in the email, I believe that the email chain is about a proposed pain clinic in Knoxville, which was to be owned and operated by SARTINI, PALMA, and RODRIGUEZ. Also, the email account **pain6100@gmail.com [7]** was listed as a contact for the HOLLYWOOD CLINIC on the clinic's Facebook page, and therefore is believed to be an account that was used to conduct clinic business.

h. Since these accounts were used to communicate about the establishment and structure of a pain clinic, there is probable cause to believe that **lucasartini@gmail.com [2], bensfmc@gmail.com [3], pain6100@gmail.com [7]** and **jimmypalmamd@gmail.com [8]** contain evidence of the crimes described in this Affidavit.

i. A review of information, from an HP Pavilion desktop computer seized from EKHCS on March 10, 2015, revealed a September 14, 2010 email chain between **nicole.sfmcdeco@gmail.com [5]** and Jennifer Allen (ALLEN), who worked for TIPTON as an administrative assistant. The **nicole.sfmcdeco@gmail.com [5]** account was reflected in the email header as "Nicole Dozier Rodriguez <nicole.sfmcdeco@gmail.com>" and most likely was used by NICOLE

RODRIGUEZ. The email pertained to the articles of incorporation of an entity in the State of Tennessee.

j. NICOLE RODRIGUEZ was listed as a managing member for MEDFIX, which was utilized by SARTINI, PALMA, and RODRIGUEZ to control the HOLLYWOOD CLINIC. NICOLE RODRIGUEZ assisted SARTINI, PALMA, and RODRIGUEZ by coordinating the establishment of a pain clinic in Knoxville, Tennessee, that was going to include an on-site dispensary. Therefore, I believe this email chain discussed the articles of incorporation regarding this proposed pain clinic with a dispensary in Knoxville, Tennessee. I believe that NICOLE RODRIGUEZ controlled **nicole.sfmcdeco@gmail.com [5]**, and that evidence of the crimes listed in Paragraph 4 of this affidavit are contained in **nicole.sfmcdeco@gmail.com [5]**.

k. A review of information, from an Acer EZ Vision laptop computer seized from EKHCS on March 10, 2015, revealed an email chain that commenced on January 24, 2013, between Maynard Alvarez (ALVAREZ), who used the email account **maynardalvarez1522@gmail.com [6],** and HOFSTETTER, who used the email account **shofstetter4@gmail.com [4]**. The email chain discussed the arrival of a new doctor and whether the doctor had received a contract from HOFSTETTER.

l. Based on this email chain, I believe that the email account **maynardalvarez1522@gmail.com [6]** is owned/operated by ALVAREZ, a defendant indicted in this matter (See Exhibit 2). I believe that this email chain concerned the employment of a medical provider at one of the pill mills operated by HOFSTETTER and owned by SARTINI, PALMA, RODRIGUEZ, and

TIPTON. Therefore, I believe that **maynardalvarez1522@gmail.com [6]** and **shofstetter4@gmail.com [4]** contain evidence of the crimes described in this Affidavit.

m. A review of information, from an Acer EZ Vision laptop computer seized from EKHCS on March 10, 2015, revealed an email chain that started on August 28, 2013, and included HOFSTETTER, who used **shofstetter4@gmail.com [4]**, SARTINI who used **lucasartini@gmail.com [2]**, and PALMA who used **jimmypalmamd@aol.com [12]**. The email chain discussed the profit and loss statements for the "Knoxville office" for 2011 and 2012. Attached to the email was a document called "Urgent Care & Surgery Center – Knoxville." This document outlined various expenses.

n. Based on the investigation, I believe that **shofstetter4@gmail.com [4]** is controlled by HOFSTETTER, **lucasartini@gmail.com [2]** is controlled by SARTINI, **jimmypalmamd@aol.com [12]** is controlled by PALMA, and that the matters they discussed concerned the Tennessee pain clinics. Therefore, I believe that all of those email accounts will contain evidence of the crimes described in this Affidavit.

o. A review of information from an Acer EZ Vision laptop computer seized from EKHCS on March 10, 2015, revealed an email chain that started on February 14, 2012, from WALKER, who used **andrew@911urgent.com [13]** to TIPTON.[2] The **shofstetter4@gmail.com [4]** account which most likely was used by

[2] The available information does not indicate which email account Tipton was using.

HOFSTETTER, who also was copied. Attached to the email was a financial statement for SARTINI that was purportedly going to be used to secure a line of credit.

p. Based on the investigation, I believe that the email account **andrew@911urgent.com [13]** was controlled by WALKER, who was the onsite accountant and business manager of the HOLLYWOOD CLINIC. Based on this email chain, I believe TIPTON and WALKER were attempting to secure a line of credit in relation to one of the Tennessee clinics. HOFSTETTER must have been involved in the transaction because she was copied on the email. Since the attempt to secure a line of credit occurred on these email accounts, I believe that **andrew@911urgent.com [13]** and **shofstetter4@gmail.com [4]** contain evidence of the crimes described in this Affidavit.

q. A review of information from an HP Pavilion desktop computer seized from EKHCS on March 10, 2015, revealed an email chain that started on October 13, 2010, from RODRIGUEZ, who used **ben@911urgent.com [14]**, to Tonya Rice, who used tonya@leveragehealthcare.com. RODRIGUEZ provided a list of email accounts to be used in the future. The email accounts RODRIGUEZ provided were **CTipton@911urgent.com [15]**, **TRice@911urgent.com**, and **KIH@911urgent.com**. Based on the timing of this communication and the names associated with the accounts, I believe these were accounts intended to be used in connection with a pain clinic in Knoxville, Tennessee, that Rice was helping to establish. A check of the 911urgent.com domain with the Internet Corporation for Assigned Names and Numbers (ICANN) revealed that the

domain was registered on May 27, 2009, and was controlled by RODRIGUEZ. Based on these facts, I believe that RODRIGUEZ caused the 911urgent.com domain to be established in connection with the pain clinic business in Florida, and that RODRIGUEZ controlled the 911urgent.com email accounts.

r. A review of information from an HP Pavilion desktop computer seized from EKHCS on March 10, 2015, revealed an email dated October 14, 2010. This email was sent from RODRIGUEZ, using **ben@911urgent.com [14]**, to Rice at tonya@leveragehealthcare.com, and contained a detailed list of items to be completed in order to open a new pain clinic in Knoxville. Since RODRIGUEZ used the account to communicate about establishment of a proposed new pain clinic, he likely discussed other aspects of the scheme on this account. Accordingly, I believe that **ben@911urgent.com [14]** and **CTipton@911urgent.com [15]** contain evidence of the crimes described in this Affidavit.

s. A review of information from a Samsung Galaxy Tab tablet computer seized from Hofstetter's residence, 1842 Falcon Pointe, Knoxville, Tennessee, on March 10, 2015, revealed a list of contacts with their corresponding email addresses, including: "Alverez Maynard" with **maynardalvarez1522@gmail.com [6]**, "Hofstetter, Syl" with **shofstetter4@yahoo.com [11]**, "Hofstetter Sylvia" with **shofstetter4@gmail.com [4]**, "Palma Jimmy" with **jimmypalmamd@gmail.com [8]**, "Palma Jimmy" with **jimmypalmamd@aol.com [12]**, "Santonocito, Filippo" with **filipposantonocito@yahoo.it [10]**, "Sartini Luca" with **luca@911urgent.com**

[16], "Sartini Luca" with **lucasartini@gmail.com** [2], "Sylvia" with **sylvia@911urgent.com** [17], and "Urgent Ben's 911" with **ben@911urgentcare.com** [14].

t. Based on the investigation, I believe that **maynardalvarez1522@gmail.com** [6], is controlled by ALVAREZ; **shofstetter4@yahoo.com** [11], **shofstetter4@gmail.com** [4], and **sylvia@911urgent.com** [17] are controlled by HOFSTETTER; **jimmypalmamd@gmail.com** [8] and **jimmypalmamd@aol.com** [12] are controlled by PALMA; **filipposantoncito@yahoo.com** [10] is controlled by SANTONOCITO; **luca@911urgent.com** [16] and **lucasartini@gmail.com** [2], are controlled by SARTINI; and **ben@911urgentcare.com** [14] is controlled by RODRIGUEZ.

u. HOFSTETTER's relationship with ALVAREZ, PALMA, SANTONOCITO, SARTINI, and RODRIGUEZ centered around the pain clinics she was operating. Therefore, I believe that all of the above-listed email accounts will contain evidence of the crimes described in this Affidavit.

v. A review of information from an Acer EZ Vision laptop computer seized from EKHS, on March 10, 2015, revealed an email chain that started on December 30, 2011, from noreply@faxtoemail.cbeyond.net to **pain6100@gmail.com** [7]. The email reads, "You have received a 20 page fax on 30 Dec 2011 at 10:51:54 AM." That same date, the message was forwarded to **andrew@911urgent.com** [13] and to **medfix@911urgent.com** [18] with the subject, "Luca's Financial Affidavit." The email was then forwarded to TIPTON in reference to a line of credit for Urgent Care Center & Surgery Center, LLC. As previously noted, TIPTON

partnered with SARTINI and others to establish pain clinics in Tennessee, and WALKER was the onsite manager at the HOLLYWOOD CLINIC. I believe this email is in reference to a line of credit associated with a proposed pain clinic in Tennessee, and that these email accounts were used by WALKER, TIPTON, and SARTINI to facilitate the transaction. Therefore, I believe that **pain6100@gmail.com [7], andrew@911urgent.com [13]**, and **medfix@911urgent.com [18]** contain evidence of the crimes described in this Affidavit.

21. A review of medical and business records seized by law enforcement from CHCS-Lenoir City on March 10, 2015, revealed the following information:

a. An email dated October 25, 2011, from "Mark Gary Blumenthal" to **shofstetter4@yahoo.com [11]** and **ctipton@leveragehealthcare.com**, transmitted a memo to HOFSTETTER and TIPTON from Blumenthal requesting payment for the company's portion of his State Volunteer Mutual Insurance Co. (SVMIC) premium. Blumenthal was medical director of CHCS-Knoxville.

b. Various checks issued by Urgent Care & Surgery Center to Mark Blumenthal in various amounts. The "For" field of the check indicated the checks were written for medical malpractice insurance.

22. I also reviewed documents obtained via Federal Grand Jury subpoena as part of this investigation. Included in that response was the following:

a. An email chain commencing on or about February 13, 2015, between TIPTON, PALMA, MASSAGLIA, and individuals associated with STERLING. The emails concerned a meeting about a proposal for STERLING to conduct urine drug

screening. The name "Sergio Massaglia" was associated with **webbankus@gmail.com [9]** in that the email address "Sergio Massaglia <webbankus@gmail.com>" **was included** in that email chain. (See Exhibit 5).

b. TIPTON, SARTINI, PALMA, and SANTONOCITO received illegal healthcare kickbacks from STERLING via GENESIS. Since this email pertains to a meeting regarding urine drug screenings, I believe these individuals would have discussed aspects of the healthcare kickback scheme by email as well.

c. Accordingly, I believe MASSAGLIA controlled **webbankus@gmail.com [9]**, and that evidence of the crimes described in this Affidavit are contained in the email account for **webbankus@gmail.com [9]**.

23. Preservation letters were issued to the Email Providers for the requested accounts. In general, an email that is sent to a subscriber is stored in the subscriber's "mail box" on the Email Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Email Provider's servers for a certain period of time.

## BACKGROUND CONCERNING EMAIL

24. In my training and experience, I have learned that the requested Email Providers provide a variety of on-line services, including email access, to the public. The requested Email Providers allow subscribers to obtain email accounts at the requested Email Providers' domain name, like the email account[s] listed in Attachments A-1 to A-4. Subscribers obtain an account by registering with requested Email Providers. During the registration process, the requested Email Providers ask subscribers to provide basic personal information. Therefore, the computers

of the requested Email Providers are likely to contain stored electronic communications (including retrieved and unretrieved email for the requested Email Providers' subscribers) and information concerning subscribers and their use of the requested Email Providers' services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. A requested Email Providers' subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the requested Email Providers. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

26. In my training and experience, Email Providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

27. In my training and experience, Email Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Email Providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

28. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. This application seeks a warrant to search all responsive records and information under the control of the requested Email Providers, providers which are subject to the jurisdiction of this court, regardless of where the requested Email Providers have chosen to store such information. The government intends to require the disclosure pursuant to the requested

warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within the requested Email Providers' possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [3]

30. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the Email Provider can show how and when the account was accessed or used. For example, as described below, Email Providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the

---

[3] It is possible that the requested Email Provider stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of the requested Email Providers. The government also seeks the disclosure of the physical location or locations where the information is stored.

time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

## CONCLUSION

31. Based on the forgoing, I request that the Court issue the proposed search warrants. This affidavit establishes probable cause to believe that each email account contains evidence of one or more of the offenses described in this Affidavit and charged in the Third Superseding Indictment in Case Number 3:15-CR-27. Because the warrant will be served on the requested Email Providers, who will then compile the requested records at a time convenient to them, good cause exists to permit the execution of the requested warrant at any time in the day or night.

## REQUEST FOR SEALING

32. I further request that the Court order that all documents filed in support of this application, including the applications, affidavits, and search warrants themselves, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, aspects of which are neither public nor known to some or all of the targets of the investigation.

Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation. A motion to seal with a proposed sealing order will be submitted herewith for consideration.

Respectfully submitted,

Steven P. Haughton
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on the 4th day of April, 2018.

Honorable Debra C. Poplin
UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A-1

**Property to Be Searched**

This warrant applies to information associated with:

**chsknoxville@gmail.com [1]**

**lucasartini@gmail.com [2]**

**bensfmc@gmail.com [3]**

**shofstetter4@gmail.com [4]**

**nicole.sfmcdeco@gmail.com [5]**

**maynardalvarez1522@gmail.com [6]**

**pain6100@gmail.com [7]**

**jimmypalmamd@gmail.com [8]**

**webbankus@gmail.com [9]**

that are stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

## ATTACHMENT B-1

### Particular Things to be Seized

**I. Information to be disclosed by Google, Inc., (the "Provider")**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 1, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1, wherever stored (See 18 U.S.C. § 2713):

a. The contents of all emails associated with the account, from in or about April 2009 through in or about July 2016, including archived, stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, and the date and time at which each email was sent;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including but not limited to address books, contact and buddy lists, calendar data, and Google calendar data;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

**The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.**

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. Section 1962 (Racketeering Influenced and Corrupt Organizations Act), 21 U.S.C. Section 841 (Illegal Dispensing of Controlled Substances, 21 U.S.C. Section 846 (Drug Trafficking Conspiracy), 18 U.S.C. Sections 1956 and 1957 (Money Laundering), 21 U.S.C. Section 856 (Drug-involved Premises), and 18 U.S.C. Section 371 and 42 U.S.C. 1320a-7b(b)(1)(A) (conspiracy to solicit healthcare kickbacks), those violations involving unknown persons, and those individuals named in this Affidavit and occurring from in or about April 2009 through in or about July 2016, including, for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

a. Tools and/or instrumentalities used in the setup, operation and maintenance of the aforementioned pain clinics in Tennessee and Florida and their associated activities, money laundering, kickback schemes, and preparatory steps taken in furtherance of the crimes listed above, as well as communication between the named parties above in furtherance of the scheme.

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;

c. Information relating to who created, used, or communicated with the accounts, including records about their identities and whereabouts.

d. The identity of the person(s) who created or used the various user IDs, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to the relevant offenses described above, including records that help reveal their whereabouts.

## ATTACHMENT A-2

**Property to Be Searched**

This warrant applies to information associated with:

**filipposantonocito@yahoo.it [10]**

**shofstetter4@yahoo.com [11]**

that are stored at premises owned, maintained, controlled, or operated by Oath Holdings Inc., a company headquartered at 701 First Avenue, Sunnyvale, CA 94089.

## ATTACHMENT B-2

### Particular Things to be Seized

**I. Information to be disclosed by Oath Holdings Inc. (the "Provider")**

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 1, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2, wherever stored (See 18 U.S.C. § 2713):

a. The contents of all emails associated with the account, from in or about April 2009 through in or about July 2016, including archived, stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including but not limited to address books, contact and buddy lists, and calendar data;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

**The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.**

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. Section 1962 (Racketeering Influenced and Corrupt Organizations Act), 21 U.S.C. Section 841 (Illegal Dispensing of Controlled Substances, 21 U.S.C. Section 846 (Drug Trafficking Conspiracy), 18 U.S.C. Sections 1956 and 1957 (Money Laundering), 21 U.S.C. Section 856 (Drug-involved Premises), and 18 U.S.C. Section 371 and 42 U.S.C. 1320a-7b(b)(1)(A) (conspiracy to solicit healthcare kickbacks), those violations involving unknown persons, and those individuals named in this Affidavit and occurring from in or about April 2009 through in or about July 2016, including, for each account or identifier listed on Attachment A-2, information pertaining to the following matters:

a. Tools and/or instrumentalities used in the setup, operation and maintenance of the aforementioned pain clinics in Tennessee and Florida and their associated activities, money laundering, kickback schemes, and preparatory steps taken in furtherance of the crimes listed above, as well as communication between the named parties above in furtherance of the scheme.

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;

c. Information relating to who created, used, or communicated with the accounts, including records about their identities and whereabouts.

d. The identity of the person(s) who created or used the various user IDs, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to the relevant offenses described above, including records that help reveal their whereabouts.

## ATTACHMENT A-3

**Property to Be Searched**

This warrant applies to information associated with **jimmypalmamd@aol.com [12]**, and that is stored at premises owned, maintained, controlled, or operated by Oath Inc., a company headquartered at 22000 AOL Way, Dulles, VA 20166.

## ATTACHMENT B-3

### Particular Things to be Seized

**I. Information to be disclosed by Oath Inc. (the "Provider")**

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of the Provider, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 1, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-3, wherever stored (See 18 U.S.C. § 2713):

a. The contents of all emails associated with the account, from in or about April 2009 through in or about July 2016, including archived, stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including but not limited to address books, contact and buddy lists, and calendar data;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

**The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.**

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. Section 1962 (Racketeering Influenced and Corrupt Organizations Act), 21 U.S.C. Section 841 (Illegal Dispensing of Controlled Substances, 21 U.S.C. Section 846 (Drug Trafficking Conspiracy), 18 U.S.C. Sections 1956 and 1957 (Money Laundering), 21 U.S.C. Section 856 (Drug-involved Premises), and 18 U.S.C. Section 371 and 42 U.S.C. 1320a-7b(b)(1)(A) (conspiracy to solicit healthcare kickbacks), those violations involving unknown persons, and those individuals named in this Affidavit and occurring from in or about April 2009 through in or about July 2016, including, for each account or identifier listed on Attachment A-3, information pertaining to the following matters:

a. Tools and/or instrumentalities used in the setup, operation and maintenance of the aforementioned pain clinics in Tennessee and Florida and their associated activities, money laundering, kickback schemes, and preparatory steps taken in furtherance of the crimes listed above, as well as communication between the named parties above in furtherance of the scheme.

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;

c. Information relating to who created, used, or communicated with the accounts, including records about their identities and whereabouts.

d. The identity of the person(s) who created or used the various user IDs, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to the relevant offenses described above, including records that help reveal their whereabouts.

## ATTACHMENT A-4

### Property to Be Searched

This warrant applies to information associated with:

**andrew@911urgent.com [13]**

**ben@911urgent.com [14]**

**CTipton@911urgent.com [15]**

**luca@911urgent.com [16]**

**sylvia@911urgent.com [17]**

**medfix@911urgent.com [18]**

that are stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

## ATTACHMENT B-4

### Particular Things to be Seized

**I. Information to be disclosed by Google, Inc., (the "Provider")**

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of the Provider, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 1, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-4, wherever stored (See 18 U.S.C. § 2713):

a. The contents of all emails associated with the account, from in or about April 2009 through in or about July 2016, including archived, stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including but not limited to address books, contact and buddy lists, calendar data, and Google calendar data;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

**The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.**

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. Section 1962 (Racketeering Influenced and Corrupt Organizations Act), 21 U.S.C. Section 841 (Illegal Dispensing of Controlled Substances, 21 U.S.C. Section 846 (Drug Trafficking Conspiracy), 18 U.S.C. Sections 1956 and 1957 (Money Laundering), 21 U.S.C. Section 856 (Drug-involved Premises), and 18 U.S.C. Section 371 and 42 U.S.C. 1320a-7b(b)(1)(A) (conspiracy to solicit healthcare kickbacks), those violations involving unknown persons, and those individuals named in this Affidavit and occurring from in or about April 2009 through in or about July 2016, including, for each account or identifier listed on Attachment A-4, information pertaining to the following matters:

a. Tools and/or instrumentalities used in the setup, operation and maintenance of the aforementioned pain clinics in Tennessee and Florida and their associated activities, money laundering, kickback schemes, and preparatory steps taken in furtherance of the crimes listed above, as well as communication between the named parties above in furtherance of the scheme.

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;

c. Information relating to who created, used, or communicated with the accounts, including records about their identities and whereabouts.

d. The identity of the person(s) who created or used the various user IDs, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to the relevant offenses described above, including records that help reveal their whereabouts.